Appendix L. Design and Implementation Issues

This appendix covers several issues that impact the development and performance of electronic commerce (EC) in the Federal government. It begins with a policy statement on the communications protocols to be employed in the virtual network (see Chapter 4). Following this is a discussion of the features on the Internet available for Federal government use for conducting electronic commerce. After this appears a section on the FTS2000 program and how it could be used. Next is a discussion of how electronic mail (E-mail) would enable delivery of EDI transactions. The appendix also covers the use of facsimile, bulletin boards, mail list servers, commercial off-the-shelf (COTS) products, electronic funds transfer, and testing.

COMMUNICATIONS CAPABILITY AND INTEROPERABILITY

The communications used by the different trading partners and the government organizations will depend to some extent on the volume of data, geographic location, and data sensitivity.

The government network entry points (NEPs) will have the capability to receive or transmit data in the following ways:

- Dedicated circuits: nonswitched point-to-point circuits that permanently connect two sites. For example, initially all of the NEPs will use dedicated circuits for communications among the NEPs.
- Switched circuits: switched circuits include circuit-switching, message-switching, or packet-switching technology. In each, connections between sites are made by one or more switches, and the connections are broken after the transmissions are completed.

The NEPs will utilize the FTS2000 services, Internet, or those available from the agency, depending on requirements, cost, and availability.

The communications software is primarily system software. The government shall avoid development of unique systems software to meet requirements; a thorough review of potential configurations (hardware and software) to meet end-to-end delivery of service must be performed prior to making a commitment to any component of the system. The intent is to ensure evolutionary increments of the system capacity and function can be met without development of unique system software.

Drawing from the recommendations of the Federal Internetworking Requirements Panel (NIST, January 1994), the basis for interworking will be based on the following hierarchy of standards:

- Open international voluntary standards (including OSI and IETF standards)
- National voluntary standards
- Proprietary or common-use standards, with a preference towards those that enjoy multinational commercial preference.

Contracts for interconnecting systems or services will include a requirement for interworking. Interconnecting parties will be held jointly responsible for interworking.

If the ISO E-mail protocol is used, it will be compliant with the 1988 (or later) version of X.400, including X.435, and compatible with the 1988 (or later) version of X.500 directory services.

NEPs shall be configurable and will be able to support the following types of connections between the gateway and the NEP: XMODEM, UNIX to UNIX copy protocol (UUCP), file transfer protocol (FTP), simple mail transfer protocol (SMTP), file transfer access management (FTAM), and X.400 transactions. (Note: the functionality supported at NEPs need not be identical depending on user requirements—it may be more efficient to route to compatible NEPs depending on the VAN and/or gateway interfaces/configuration.)

THE INTERNET

The government continues to support the development of both the Internet and the open systems interconnection (OSI) protocol suites. While the X.400 mail can be supported with the underlying Internet protocol suite (IPS), most of the X.400 systems have been implemented with CLNP (CLNP is the OSI IP standard Internet protocol designed to be used with X.25). In SMTP and

MIME, the IPS-based E-mail service has been implemented with TCP/IP.

The OSI protocol suite and IPS have created a competitive environment that has fostered similar, but not equivalent, enhancements to both suites. The Multipurpose Internet Mail Extensions (MIME) provides similar IPS capabilities to that afforded through the use of the X.400 UA P2 protocol.

The IPS currently needs additional security before being used for business transactions. There are significant efforts underway to eliminate deficiencies inhibiting the use of Internet for business transactions. In November, under the Technology Reinvestment Project, a $8 million contract was awarded to Enterprise Integration Technologies, the Center for Information Technology at Stanford University, and BARRNet, a regional Internet access provider. The intent of the project is to address the security, performance, and ease of use problems which could prevent the Internet from being used for commerce. Based on current government policies and funding, government systems intended to support resource sharing for several different organizations must not only support both suites, but be capable of the transition between protocol suites.

The Internet is one way to provide connectivity among agencies, with participating VANs, and with the public sector that is either directly or indirectly connected to the Internet. The Internet is the system of interconnected computer networks that share the protocol suite and the name and address spaces that are specified by the Internet Architecture Board (IAB) of the Internet Society (Postal, October 1993; Reynolds, 1992). The IPS is defined in publicly available papers called request for comments (RFCs). While a few of the RFCs have achieved the status of standard and are required of any network that is to be attached to the Internet, most RFCs are working papers use within the Internet community to describe ways to add new function or to address problems discovered in real world operations. Today, the Internet has over 21,000 connected networks, supporting an estimated 20 million users worldwide (Widmeyer, 1993). This success is the source of some of the issues with using the Internet. Can the Internet cope with it rapid growth? Other issues, some of them based on misconceptions, include reliability, security, ease of use, and payment.

While it is true that the Internet is running out of IP addresses, this problem is being addressed. The Internet

Engineering Task Force (IETF) has proposed a temporary solution that increases the efficiency with which addresses are used and should last until the end of the decade. At some time in the future, it will be necessary to add digits to the IP address. This is somewhat like the U.S. phone system, which has run out of numbers several times and is headed that way again. Ten years ago local calls were dialed with 7 digits; today, in some metropolitan areas, local calls now require dialing 10 digits.

The question of reliability in the Internet is one that can be addressed on two levels. First, an underlying design requirement for TCP/IP was survivability in a hostile environment; ARPANET was a DoD project after all. Second, the owners/operators of individual networks connected to the Internet can make their own arrangements (redundant links, etc.) to achieve a level of reliability and availability as necessary.

Much of the security exposure associated with the Internet is in fact related to the specific implementations and configuration management practices at individual host systems. The solution to break-ins rests with the host system administrators. There are a set of RFCs (Privacy Enhanced Mail RFC 1421-1424) that address issues of message authentication, confidentially, and signature. Many of the important Internet management protocols also have security features defined. However, none of this is widely deployed because of a lack of a system for key management. The problem is not one of technology or of design, but rather the lack of progress on the policy issues of cryptography, key registration, certification, key escrow, export control, digital signature standards (including certification), and patent ownership. Until these policy issues are resolved, there can be no expectation of a secure internetworking solution of any sort. A network can decide on a security methodology but there is no such consensus between networks. A national public key registration and certification infrastructure (PKI) is a prerequisite to secure messaging.

Ease of use is central to effective network operations and end-user acceptance. Internetworking is not a simple process, and day-to-day operations require coordination and cooperation among participants. The market place seems to be moving towards a second generation of the IPS Simplified Network Management Protocol (SNMP 2) as the tool of choice. Electronic mail demonstrates this contrast in end-user acceptance aspect between IPS addressing and ISO X.400 addressing. X.400, by requiring that the ADMD portion of the O/R address be specified, effectively requires the sender to know the communications carrier (VAN) of the recipient. While widespread implementation of X.500 directory services should mitigate some of the problems (e.g., allowing ADMD to be blank), no such service is now available. Indeed, the largest worldwide X.500 directory pilot is available through the Internet.

The issue of cost centers around the questions of subsidy, price and payment. As to subsidy, three points should be made:

- VANs perceive it as unfair.
- Others believe that, since the taxpayers are footing the bill for the core (backbone) of the Internet, the government should benefit from its availability.
- The subsidy is being reduced anyhow.

The Internet is being commercialized, evidenced by the growth in VANs that base their operation on the IPS and the Internet. As to price, except for the backbone, most of the cost of participating in the Internet is borne directly by the participating entity. They also bear part of the cost of the backbone through access fees. With the continuing reduction in direct government support, the Internet is becoming increasingly commercialized. Appropriate use policies are all but gone (except for those imposed by the collective user community). The commercial Internet should continue to play an important role as a model for the development of useful internetworking and cost recovery, and as an competitive challenge to limited interoperability offerings from other sources.

To fully appreciate this, one should contrast the location of the service providing computers (hosts) in the Internet with that of VAN provided services. In general, an origination that provides Internet access for its employees also provides the computers, storage, gateways, routers, and software; in other words, almost all of the functionality. How this is accounted for internally is up to the enterprise. VANs however have to carry most of the capital investment and operating cost of the service they provide. The way VANs chose to price their services tends to reflect a telephone model of "sent paid" messaging with the originating VAN collecting and keeping all of the revenue. This election by the VAN community creates the need for a settlements process whenever VANs exchange traffic, which in turn creates a business barrier to interworking on top of the technical and operational barriers. Since the Internet community has selected to provide most of their function internal to their organization and to pay for the backbone through fixed monthly access fees, they have avoided the expense of account for interorganization communication. There is a linkage between cost and usage even in this case; higher speed access to the backbone cost more.

While the services associated with the IPS can provide a first step towards meeting the President's July 1994 milestone, significant work remains to be done before the Internet itself can fully support the EC initiative. Some of the Internet features usable for EC today include E-mail with enhancements, file transfer, bulletin boards (moderated and open), and mailing list servers. A key missing function is the explicit support for X12/EDIFACT messaging. Members of the IETF have established a formal work group to address this.

The capabilities for finding other users and data within the Internet are not widely appreciated outside the Internet community. The following identifies and discusses searching features commonly available (the material is drawn from a Draft Working Paper by Jerry L. Johnson, Texas Department of Information Resources, with additions):

- **WHOIS++** — a tool for looking up users in directories (also known as “White Pages”). Whois++ makes sense as a local directory service. The implementations are small and install quickly, and the raw query language is simple. The simplicity of the interaction between the client and the server make it easy to experiment with and to write clients for, something that wasn't true of X.500 until LDAP. In addition, Whois++ can be run strictly as a local service, with integration into the global infrastructure done at any time. It is true that Whois++ is not yet a fully functional “White Pages” service. It requires a lot of work before it will be so. However, X.500 is not that much closer to the goal than Whois++ is.
- **NETFIND** — a tool for locating items within the Internet. Right now, the “White Pages” service with the most coverage in the Internet is Mike Schwartz' Netfind. Netfind works in two stages: find out where to ask, and start asking. The key feature of Netfind is that it is proactive. It doesn't require that the system administrator bring up a new server, populate it with all kinds of information, keep the information in sync, worry about update, etc. It just works.

- **ARCHIE** — a tool for finding the location of public files in the Internet. A user enters on a command line a simple search request for a file by name and the Archie process connects to known public file archives and searches the archives' directory for a match. Archie is a success because it is a directory of files that are accessible over the network. Every FTP site makes a "conscious" decision to make the files available for anonymous FTP over the network. The mechanism that archie uses to gather the data is the same as that used to transfer the files. Thus, the success rate is near 100 percent. In a similar vein, if Internet sites decide to make white-pages data available over the network, it is possible to link these servers to create a worldwide directory, such as X.500, or build an index that helps to isolate the servers to be searched, Whois++. Users don't have to do anything to their FTP archives to have them included in archie.

- **FINGER** — The Finger program, which allows one to get, from a host running the server, information about an individual with an account or a list of currently logged-in users, can be used to check a suggestion that a particular individual has an account on a particular host. This does not provide an efficient method to search for an individual.

- **GOPHER** — provides a menu-driven tool for searching and retrieving from file directories. Sites that wish to make certain files available on the Internet prepare a directory structure that aids in the organization and access to the offered items. The directory structure is represented by menu pages that contains text describing each level or entry in the hierarchy. A Gopher server is run which allows controlled access from users with Gopher client programs. The types of data available include the National Performance Review broken out chapter by chapter and text for White House speeches. Pacific Bell (the California telephone company) runs a Gopher server where documents about their new network field trials can be found. A gateway between Gopher and X.500 has been created so that one can examine X.500 data from a Gopher client. Similar gateways are needed for other White Pages systems.

- **World Wide Web (WWW)** — another Internet "navigation" tool for finding and getting data. This tool allows a user to find and access documents and then to follow "hyper-text" links from one document to another. The documents need not be at only one site. One can traverse the Internet going from network site to network site as they follow the links in one document to another.

- **MOSAIC** — Mosaic for X Windows was developed by the National Center for Supercomputing Applications (NCSA) and provides a public implementation of the software. Mosaic provides a Graphical User Interface (GUI) that facilitates user access to information on the Internet. Mosaic provides a graphical interface to the WWW and hypertext based information and other linked index/directory services such as Archie, FTP sites, Gopher, and X.500 directory information. Mosaic also supports on-line Graphic Interchange Format (GIF), Joint Photographic Experts Group (JPEG), Motion Picture Experts Group (MPEG), QuickTime, and other document, image, and audio types.
- **VERONICA** — Very Easy Rodent-Oriented Netwide Index to Computer Archives. VERONICA allows a user to search Gopher menus (see Gopher) to locate information by searching for words in the descriptive text.
- **WAIS** — Wide-Area Information Server. WAIS allows full text searches of a document for keywords. WAIS resources are indexes and its value as a search engine as very much dependent upon the quality of work done by the indexer. Like other Internet tools, WAIS allows one to search indexes and access documents without concern as to their actual location within the net.

The Federal government's electronic commerce initiative will work best when there is a reasonably reliable, reasonably trustworthy (comparable to the USPS) interworking electronic communications system that appears as ubiquitous and as easy to address as the telephone system. Collectively, the community of service providers using X.400/500 has not yet been able to satisfy the interworking objective. The Internet comes closer to the goal of wide coverage and interworking, but it to has a way to go since it does not yet support the E-mail enabled EDI.

FTS2000 PROGRAM

The Federal Telecommunications System 2000 (FTS2000) program provides intercity telecommunications services for Federal government users. The FTS2000 contracts were awarded by the General Services Administration (GSA) in December 1988 and will expire in December 1998. GSA has initiated efforts associated with defining concepts for government telecommunications provisioning in the post-FTS2000 environment. Part of this effort involves assessing the current and emerging telecommunications technologies and Federal agency requirements over the next 15 years. The assessments of technologies and requirements through the year 2008 is being accomplished without regard to the constraints and assumptions particular to the existing FTS2000 program.

FTS2000 SERVICES

Under the current FTS2000 contract, two contractors, AT&T and Sprint, each provide the following six basic CONUS telecommunications services:

- Switched voice services (SVS) and low-speed data transmission capabilities up to 9.6 Kbps are available. FTS2000 to FTS2000 calls are completed by dialing a 10-digit number. Users can access the FTS2000 network via on-net, virtual on-net, or off-net access facilities.
- Switched data service (SDS) resembles SVS, except that the access lines are specifically conditioned to carry data traffic. High-speed data transmission requires special equipment and access circuit conditioning. SDS is provided at 56 Kbps or clear channel at 64 Kbps.
- Packet-switched service (PSS) has an access capability up to 56 Kbps. The networks are designed to support a range of user devices operating at different speeds, and with different protocols. The networks support interconnection of a variety of asynchronous and synchronous terminal devices and computers by segmenting data into packets, which are forwarded to their ultimate destination through the path of least delay. The packet switched service is being enhanced to provide increased throughput by elimination of error checking within the network; this frame relay permanent virtual circuit service provides speeds up to 1.545 megabits. FTS2000 PSS features and capabilities include electronic mail and telex. The electronic mail service includes electronic bulletin boards, and electronic forms generation.
- Video transmission services (VTS) are available in two modes: compressed video transmission service (CVTS) and wide-band video transmission service (WVTS). Both services offer point-to-multipoint broadcast and two-way video communications with synchronized audio and video signals for simultaneous reception. WVTS is provisioned over satellite facilities, and is used primarily for point-to-multipoint video broadcast applications.

- Dedicated transmission service (DTS) offers user agencies unlimited point-to-point nonswitched service at a fixed monthly charge. DTS lines can support the other services such as voice, data, or video subject to line quality or capacity limitations. There are five basic DTS offerings available to the government: 4.8 Kbps analog, 9.6 Kbps analog or digital, 56 Kbps analog or digital, 1.544 Mbps (T1 service) digital access and transport, and 45 Mbps (T3 service).
- Switched Digital Integrated Service (SDIS) provides integrated access to on-net SVS, SDS, PSS, CVTS, and DTS. Primarily SDIS provides a pricing option for the government. In many scenarios, SDIS will offer cost savings to the government. Both contractors offer ISDN provisioning of services at locations with compatible equipment.

STATUS AND ENVIRONMENT OF MANDATORY FTS2000 SERVICES

FTS2000 services are available to all Federal government organizations. The states and local governments have been allowed to use FTS2000 services only if they have a sponsor who is a Federal user. The FTS2000 contract is mandatory for Federal agencies with a few exceptions. The Department of Defense uses FTS2000 services that meet its requirements. Analysis has indicated that the contract is cost effective and allowing many exceptions could easily lead to reduced volumes, which would impact the overall effectiveness. The contract is not a requirements contract, but guarantees a specific level of revenue, which has already been met. Further, the use of FTS2000 services such as DTS with enhanced services of another vendor (not part of FTS2000 contract) has been treated as acceptable use. For example, an organization might use DTS services and add packet switched capability from another vendor if this arrangement were cost effective. The primary purpose of FTS2000 was to provide transport capability.

The initial planning for the follow-on for the FTS2000 contract is still in the early stages; however, a Federal working group reviewed requirements and expected applicable technologies. Its report, "Networking for a Reinvented Government: Federal Telecommunications Requirements and Industry Technology Assessment," indicates the need for a flexible contract that takes into consideration the rapid changes in technologies; one would expect a much shorter contract life than the current FTS2000 contract. However, the limited infrastructure of many Federal organizations and the expected cost of duplicate contracts provides reasonable assurance that a government-wide follow-on to the FTS2000 contract will be pursued. Expectations are that the breadth of services will be much broader with potentially more choices of vendors; however, another Federal working group is formulating the acquisition approach, and their recommendations will not be available for several months.

IMPACT OF THE FTS2000 CONTRACT ON EC

Based on previous interpretations and the current practice, a principal role for FTS2000 in the implementation of EC would be mandatory transport services purchased by the government. FTS2000 involvement is a function of the communications needed to meet the necessary connectivity between the government and its trading partners and the supporting VANs. If the government is expected to pay for the long-haul communications charges, then the communications services should be supported and acquired from the FTS2000 contract. The availability of X.400 E-mail services on the FTS2000 contract with a supporting communications infrastructure and the executive mandate for ubiquitous E-mail service in the government justifies extensive use of the FTS2000 contract for Federal agencies to develop an EDI X.400 infrastructure.

The government wants to encourage development of EC technology both in government and industry. If only some of the trading partners are EC capable, then provisions are needed to support two different approaches for handling transactions from the trading partners: one for EDI and the other for non-EDI. Hence, the availability of the necessary support for a trading partner to meet the requirements to interface to the government via the use of EDI is needed to maximize competition and to reduce the government's operational cost. Furthermore, the government will not be able to refuse to do business with companies because they are not EDI capable unless the cost difference to the trading partner is significant. Hence, the government will probably have to ensure trading partners have an option to access EDI services for costs which are no greater than their current mode of operation. If so, the government needs to ensure that industry provide that service with minimum government intervention and expense.

Limiting the number of companies providing VAN services will most likely increase cost to the trading partners, inhibit the availability of VAN services, and delay many trading partners from the transition to an EDI capability. The selection of a single

VAN to serve the Federal government could restrict the growth of EDI and inhibit competition. The multiple VAN arrangement described in the various network architecture alternatives maximizes the governments ability to attract and reach potential suppliers. This is particularly true as VANs specialize to meet the needs of particular industry segments. This approach provides all VANs with an equal standing and access to Federal procurement actions. The multiple VAN approach maximizes the business opportunities for small business, and reduces the need for Federal agencies to recruit trading partners.

E-MAIL ENABLED EDI

One of the goals of the executive branch of the government is to create an infrastructure to support ubiquitous E-mail to serve the government, public sector, and industry. If properly implemented, this same infrastructure can also support electronic document interchange. As an alternative to the standard ASC X12.56 protocols, E-mail can be an attractive way to send near real time transactions without waiting to use the batch-oriented transactions of ASC X12. Based on the planned underlying protocol structures there are three primary options for E-mail support: X.400, particularly X.435; the simple mail transport protocol (SMTP); and the Multipurpose Internet Mail Extension (MIME). E-mail provides an excellent method for transporting ASC X12 transactions. The X.500 directory provides the capability to dynamically resolve addresses which significantly enhance the EDI functionality of electronic mail. Additionally, compliance with X.435 enhances the capability of OSI based networks to support electronic commerce; the X.435 format enables the application to transmit electronic messages or ASC X12 transactions in the same session. MIME, as the name suggests, is an extension to SMTP and is being considered within the Internet as the mechanism for specifying and describing the format of Internet message bodies. MIME enables the Internet to deliver complex data needed for multimedia through the E-mail.

Perhaps the most persuasive argument for emphasizing the E-mail route to the "single face to industry" goal is that EC involves more than the interchange of transaction data sets. The totality of a contractual relationship involves also the textual communications surrounding shipping and delivery arrangements, billing and payment inquires, damaged goods and rework issues, etc. Until, and even after, implementation conventions are established for these messages, an interpersonal messaging system will be required. We believe that a “single face to industry” is supported when a supplier can use one set of procedures for electronic interaction to receive and send EDI transactions and the same set of procedures, interface, and service provider to conduct the concomitant dialogues.

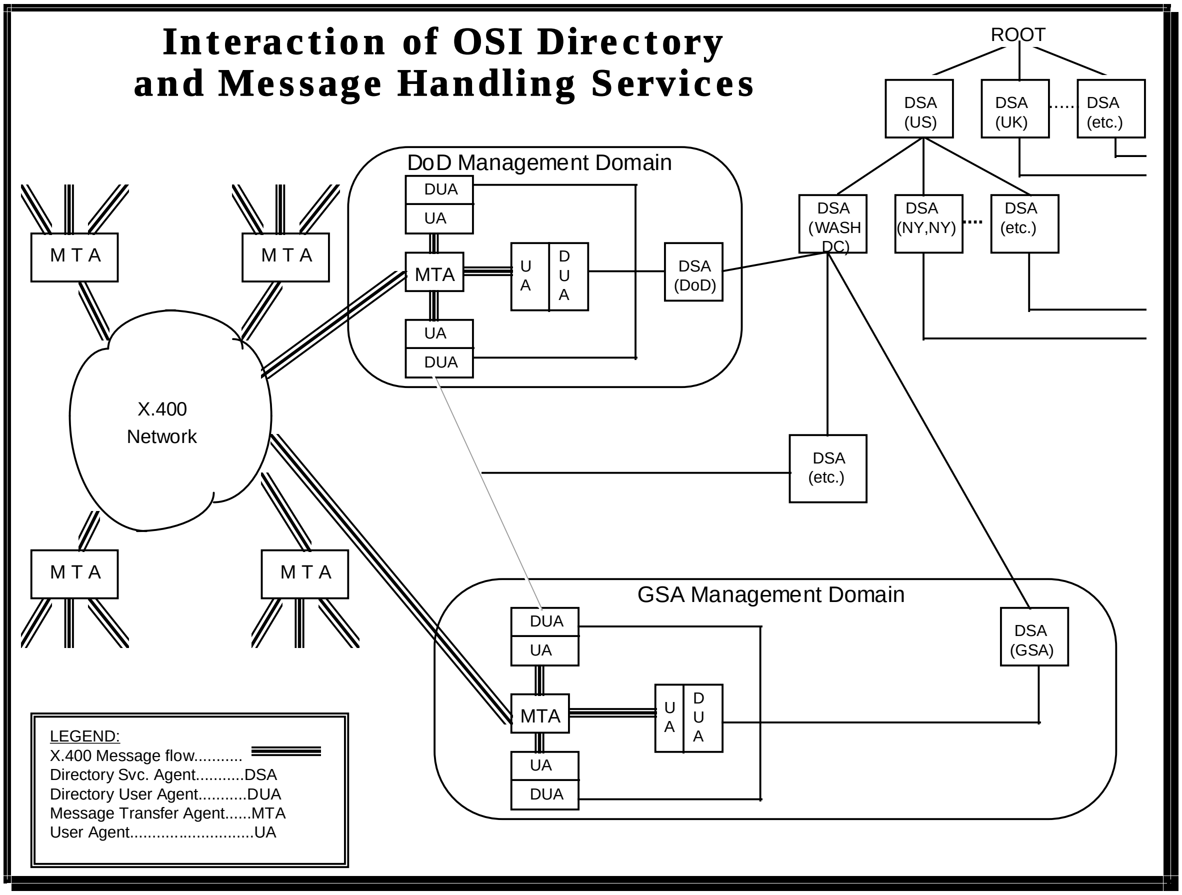

Interaction of OSI Directory
and Message Handling Services
ROOT
DSA (US)
DSA (UK)
DSA (etc.)
DSA (WASH DC)
DSA (NY,NY)
DSA (etc.)
DoD Management Domain
DUA
UA
MTA
U A
D U A
DSA (DoD)
UA
DUA
M T A
M T A
X.400 Network
M T A
M T A
DSA (etc.)
GSA Management Domain
DUA
UA
MTA
U A
D U A
UA
DUA
DSA (GSA)
LEGEND:
X.400 Message flow...........
Directory Svc. Agent...........DSA
Directory User Agent...........DUA
Message Transfer Agent......MTA
User Agent............................UA

Figure L-1. Interactions of X.500 Directory Services with X.400 Message Handling Systems

Figure L-1 shows the interactions of X.500 directory services with X.400 message handling systems. The basic components of a message handling system can be divided into the following: management domain, message transfer agent, message store, and user agent. In this respect, the X.400, SMTP, and MIME environments are similar. The basic structure of the X.400 environment will be described, and to some extent contrasted with SMTP and MIME.

There are two types of management domains: public and private. The public domains are called administrative management domains (ADMDs) and private domains are called private management domains (PRMDs). PRMDs normally are associated with an individual organization, whereas the ADMDs service many different and possibly unrelated organizations. The addressing within the domain is managed locally; however, the ability to move a message to a different domain requires the message to be forwarded to a local interface. A message going to a different domain will use a message transfer agent (MTA, protocol P1, X.400) to reach the interface entity that determines the next hop of the route. The interface entity maps the message and header routing lists into the correct format for the receiving MTA. The interface may use a directory service such as X.500 to determine the OSI (connectionless network protocol—CLNP) or Internet (IP) address depending on which protocol suite is being used. The X.500 model has a global perspective which views the world as a single domain composed of many subdomains cooperating and interconnecting.

A VAN may be an ADMD that provides an E-mail service using a long-distance communications network for the transport capability. VANs can be, and frequently are, interconnected, which provides a potential path between remote E-mail users. Today, X.400 (88) addressing (O/R addressing) requires that the sender of a message know and include the name of the recipient's VAN, that is, the ADMD name of the VAN that services the destination. This requirement makes O/R addressing harder to use than other addressing schemes. It also makes it more difficult for vendors to change VANs in an otherwise competitive marketplace. Electronic commerce needs MTA implementations that are capable (most likely thorough the use of X.500 directory services) of accepting and delivering messages without a sender provided explicit ADMD.

The user agent (UA) provides an interface between users and their E-mail environment. The UA, with assistance from the MTA, allows the users to send and receive data with another E-mail user; separate mail boxes should be established for EDI transactions. User agents are identified by the structure they support. In 199l, a formal UA was defined for EDI; this user agent requires a recently defined protocol called P35 or Pedi. This protocol is similar to another UA protocol called P22 (enhanced P2 for 88 version X.400) which supports multimedia.

ATTACHMENTS AND CHARACTER FORMATS

The P35 format has additional services to ensure the validity and integrity of the message as a business transaction. Although not widely implemented, the most basic UA protocol, P0, can accept X12 transactions and convey them through the X.400 mail. Current government E-mail implementations which plan to support EDI transactions before 1996 should implement P2 as the preferred approach. It is anticipated that X.435 which requires implementation of P35 will be widely used by industry and should be mandatory for government installations by 1996.

The message store concept was added to the standards in the 1988 X.400 specifications. This includes the concept of temporary storage facilities which allow waiting until a system is able to retrieve the message.

NON-EDI TECHNOLOGIES

The objective of EDI is to facilitate business transactions that can be performed independent of human intervention. However, there is a need to support transition from labor intensive functions as expeditiously as possible. Hence, there will be some functions of a business process which will need some human intervention to ensure an expeditious transition can be performed and still maintain continuity of services.

FACSIMILE

The intent is not to include fax support as part of centralized EDI applications. However, a government organization or a VAN may use fax in order to move part of an application into an EDI environment. For example a VAN may support a trading partner by going from ASC X12 transactions to fax for output, and on the input side perform optical scanning of fax information, and convert this information into ASC X12 transactions for government processing. Individual government organizations may perform functions as needed to facilitate EDI applications; however, these functions should be hidden from the standard centralized EDI processing.

BULLETIN BOARDS

Bulletin boards can be used effectively to minimize telecommunication cost, and transfer responsibility for inquiries to non-government personnel. For example, the NEPs will send all new RFQs to the VANs, and it is their responsibility to ensure that each of their customers, regardless of communications facilities, have an opportunity to review the RFQ the same day it is released. Some VANs will have the capability to establish and manage bulletin board type systems that support ASC X12 transactions and allow sorting and serach capability. This allows vendors an efficient way of browsing through the potentially long list of RFQs and examining only those of interest; for example, vendors that do not sell pencils will not be interested in examining RFQs for pencils. Still another advantage is that vendors have the option of searching the bulletin boards at their convenience based on current needs and requirements without receiving all RFQs issued. Viewed from a different vantage point, searching a bulletin board at a convenient time requires vendor initiated action. Some VANs offer other types of services to disseminate public information. Using a VAN, vendors can have RFQs delivered directly to their mail box without the need to initiate any action. Furthermore, VANs may provide vendors additional services such as EDI translation, and delivery of only selected RFQs based on product categorization. Of course, there will be a cost to vendors for these services that must weighed against the benefits they offer.

MAIL LIST SERVERS

The use of mailing lists may be particularly convenient for those with access to the Internet. These could be set up based on geographic location, product categorization, or any other grouping where there is a shared interest. Again, tools to automate searching or provide additional services could be implemented. To make use of mailing lists, one or more lists could be created for this purpose. All that is required is a system that supports an electronic mail service. The electronic mail system creates an “alias” that results in substituting a single electronic mail address for the electronic mail address of multiple users. Architecturally, a mailing list can be viewed in the same way as a VAN. RFQs would be sent to the mailing list and this would result in it going to many vendors, in much the same way that an RFQ sent to a particular VAN ends up being delivered to many vendors. The details of how this is handled in either situation are not of any particular importance to the overall architecture.

COMMERCIAL OFF-THE-SHELF PRODUCTS

COTS products are preferred over government off-the-shelf (GOTS) products or the development of a product. COTS products have the advantage of being used in different environments and supported by a nongovernment staff. With a large user base, fewer software problems are likely. Also, COTS products provide maintenance under maintenance agreements with the software provider. In the case of COTS software products, source code must be placed in escrow in case of the business failure of the supplier.

If no COTS products are available to perform a given function, GOTS products are preferred over the development of a product. GOTS products may or may not be supported by a the government entity that sponsored the development. In the case of the former, the government entity should be reimbursed for performing maintenance functions. In the case of the latter, the necessary documentation should be acquired so that maintenance can be performed either by government personnel or by a contractor. In the case of GOTS software products, source code must be obtained from the sponsoring government entity.

Product development will only be undertaken when no COTS or GOTS products exist that can be modified to meet the requirement.

ELECTRONIC FUNDS TRANSFER (EFT)

Upon the approval of invoices from vendors, each department or agency will issue a payment order to its payment office [either the Treasury or the Defense Finance and Accounting Service (DFAS)]. Using the information provided by the payment order, the payment office will initiate an electronic funds transfer (EFT) to the designated bank. Upon receipt of the EFT, the bank sends a credit advice to the vendor for the amount of the funds transferred. All security provision for EFT are consistent with the banking industry standards (ANSI X9).

FEDERAL RESERVE BOARD NETWORK

The Federal Reserve Board (FRB) network is the network of banks that transport EFTs. This network is called the automated clearinghouse system (ACHS). The only Federal government organizations that may generate funds transfers over this network are the Department of Treasury, the Defense Finance and Accounting Service, and the Department of State.

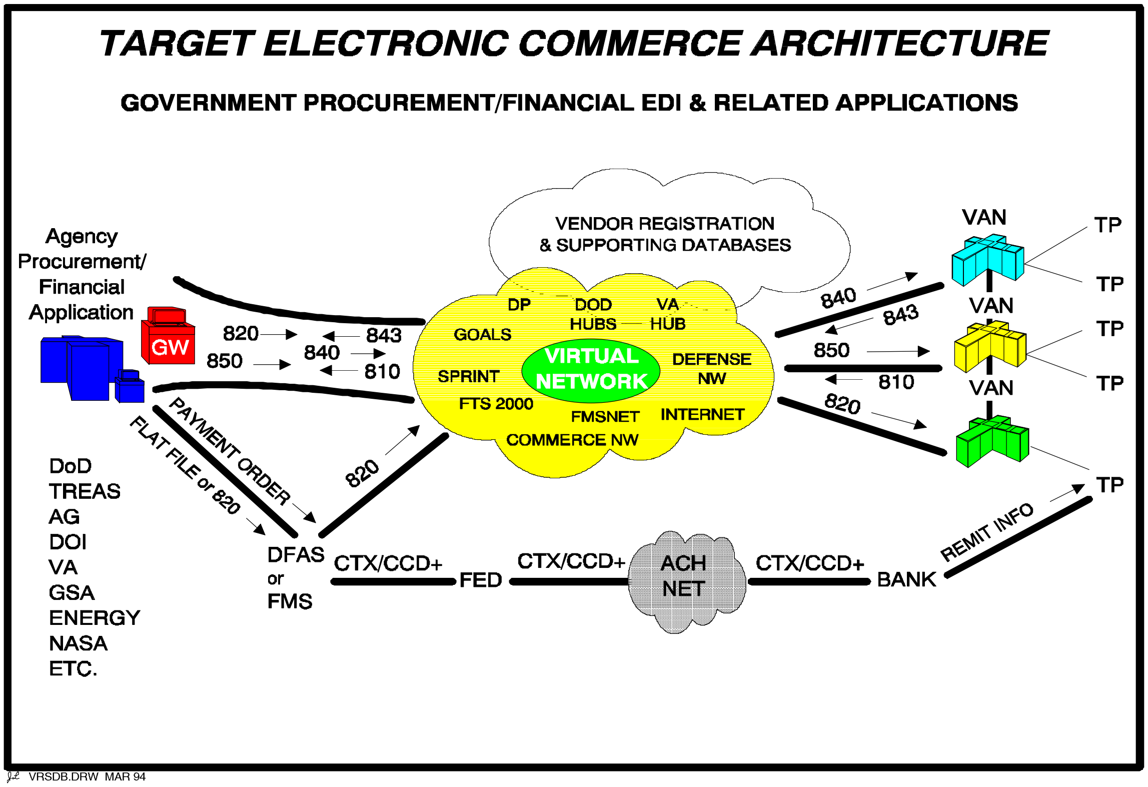
DEPARTMENT OF TREASURY

The Department of Treasury (FMS) receives X12 transactions for payment by various methods. Upon receipt, the FMS may generate the necessary EFT for transport over the ACHS.

DEFENSE FINANCE AND ACCOUNTING SERVICE

The Defense Finance and Accounting Service (DFAS) receives notice for payment through the DoD agency network, the Defense Information Systems Network (DISN). Upon receipt, the DISN may generate the necessary EFT for transport over the ACHS.

Payment orders and EFT transaction do not use the EDI network. The transactions occur directly between the procurement office and the payment office.



VRSDB.DRW MAR 94

Figure L-2. Target Electronic Commerce Architecture

INTERNATIONAL TRADE

United Nations World Trade Point Centers (InfoPort) could serve as a proponent of EDI and international commerce. InfoPorts are planned to be worldwide, nonprofit, and not in direct competition with commercial providers of other services. As a neutral party, they may serve as a Trusted Third Party, depending on the security and related services they provide. InfoPorts are still in development and will be available for pilot initiatives in 1994.

ADDITIONAL OPPORTUNITIES

It is worth noting that while the application driving the development of this architecture is acquisition, the resulting communications and shared data base capabilities will be relevant to other areas. Potential Federal users include any of the government's social programs that involve some form of claims processing (e.g., SSA, student loans, health care, VA, etc.), any program that involves an information request (as defined by the Paperwork Reduction Act), or any of the numerous financial/tax reporting application are all potential users. The capability can be extended to include state and local governments, particularly where they are responsible for the day-to-day operation of Federal programs (e.g., unemployment insurance, state taxes, food stamps).

TESTING

Given the large number of participants that will be involved with EC, there arises the question of what works with what. Issues of known importance include E-mail and X12 address mapping, inter-VAN interworking, directory services, complex document representation and transfer, and message security.

INTERNAL GOVERNMENT EC TESTING

The capability to successfully perform EC is dependent on the exchange of ASC X12 transaction data and interpersonal messages among the Federal users, NEPs, VANs, and the trading partners. The efficient and proper delivery of the transactions is dependent on a telecommunications infrastructure that provides the necessary communications topology, compatible protocols, and a supporting addressing structure. A set of tests is needed to verify that the communications infrastructure provides the required interworking. The communications infrastructure used to support end-to-end delivery frequently is performed by a series of sessions that are not necessarily concurrent. Therefore, the communication sessions and the ability to transverse the different communications sessions must be verified. The EC testing responsibility includes the transfer of data from the agency system to the VAN. A trading partner to perform EDI is dependent on the government's agency system and also the trading partner's own application. There will be government application systems such as NEP data base support which will be integral to EC, and the required testing is an EC responsibility. These supporting applications shall be tested as individual components, followed with integration and system testing. The communications infrastructure tests will be separate from the application tests, but the communications infrastructure may be required to perform application system testing. Hence, testing will include component testing, integration testing, and system testing. The principles of regression testing will be standard practice.

VAN ACCEPTANCE TESTING

Before any VAN can utilize the government's facilities it must submit an implementation plan that identifies the extent of the proposed participation and that includes the conventions intended for use. The conventions must be agreed to by the corresponding government organization and be consistent with a set of conventions approved by the government. The plan will identify the intended protocol suite and the government entities that will be participants:

- The gateway will establish testing procedures to verify the ASC X12 transactions and conventions independently of the communications.
- The government will develop and conduct tests to verify that the VAN can perform the communications independent of the specific application. The VAN must satisfactorily complete these tests prior to certification.
- Once the VAN has passed the communications and applications (X12 transactions) tests, it must also complete a set of end-to-end tests (performance criteria) before certification. The specific transactions tested will be mutually agree to by the VAN and the government.

RECOMMENDATIONS

Achieving the following objectives are essential for a successful ubiquitous government EDI capability:

- E-mail systems may be used as the transport medium for EDI transactions.
- FTP, FTAM, SMTP, X.400, or X.400 compatible substitutes are the preferable transport methods for EDI.
- EDI functionality must be supported such that the user can choose between IPS and OSI protocol support.
- Directory services will be provided through the X.500 model as services become available.
- Initial implementation of X.400 shall support the user agent services defined in P2 and P22 protocols.
- By 1996, the X.400 implementations shall contain the services defined in the X.435 specification.
- The Internet network may be used for EDI transactions when it is capable of providing the essential reliability, security, and privacy needed for business transactions.